高品質なソフトウェアを速く、安く、正確に作る

田原 研究室

田原 康之
Yasuyuki TAHARA

現代のモノづくりはソフトウェアが鍵を握っているといっても過言ではありません。携帯電話やデジタル家電、自動車、医療機器などには「組み込みソフトウェア」が搭載されています。ハードウェアに対して、ソフトウェアはプログラムによって書き換えられるため、機能の追加や変更が容易です。ソフトウェアの導入によってモノづくりは高性能化し、開発スピードも格段に向上しました。

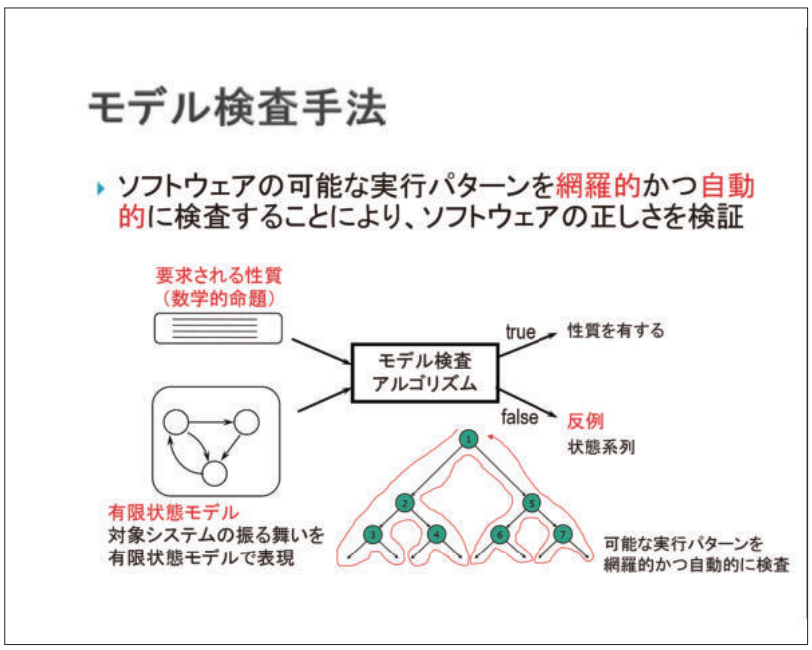
しかし、ソフトウェアは近年、大規模化が進み、プログラムが複雑化してソフトウェア開発に必要なコストが膨らんでいます。ソフトウェア産業では人海戦術で乗り切る傾向がみられますが、それも限界があります。大勢のチーム作業はマネジメントも難しく、刻々と移り変わる市場ニーズも常にくみ取らなくてはなりません。

ソフトウェア工学

これらの課題を解決する学問が「ソフトウェア工学」です。ソフトウェアをいかに速く、安く、高品質に作るか——。ソフトウェア工学はこうした目的を達成するため、数理論理学などの高度な数学の理論を駆使し、有益なソフトウェアの開発を目指すアプローチです。プログラムの作成には人間の知的活動が深く関わっています。そのため、心理学などの人文・社会科学とも決して無縁ではありません。

ソフトウェアは人間がプログラミングして作るため、曖昧な部分が多く、そこに間違いがあればバグ(欠陥)となって装置の誤動作などを引き起こします。人間の曖昧さと、記述通りのプログラムでしか動かないコンピュータとの間に大きな溝があるのです。

従来は複数の目でチェックしたり、テストデータを入力したりして動作を確認していました。しかし、プログラムのすべての動作をチェックすることは現実的ではありません。そこでソフトウェア工



キーワード

ソフトウェア工学、形式検証(モデル検査)、要求工学(ゴール指向要求分析)、セキュアなシステムの開発手法、ソフトウェア基礎理論(圏論、代数モデル、形式的意味論)

所　属	大学院情報理工学研究科 情報学専攻
メンバー	田原 康之 准教授
所属学会	情報処理学会、電気学会、 日本ソフトウェア科学会
E-mail	tahara@uec.ac.jp

学の手法を使い、厳密な数学の理論に基づいてプログラムの正しさを網羅的に確認するのです。

モデル検査を適用

ソフトウェア工学が専門の田原康之准教授は、ソフトウェアの仕様の記述や設計、検証のための「形式手法（Formal Methods）」と呼ばれるツールを使っています。その中でも特に、ソフトウェアの仕様に対して網羅的かつ自動的にプログラムを検査する「モデル検査」手法を使いこなすエキスパートです。

具体的には、グーグルマップなどに使われているウェブアプリケーションの代表的な開発手法である「Ajax（エイジャックス）」にモデル検査を適用する研究を進めています。Ajaxは操作性が高い反面、動作が複雑でバグが発生しやすい問題点があります。田原准教授はAjaxに初めてモデル検査を導入し、プログラムのバグをほぼ自動で迅速かつ正確に見つけ出すことに成功しました。

モデル検査は一部で実用化されつつある手法ですが、今後、Ajaxなどの汎用技術に本格的に導入されれば、その方式が瞬く間に普及するでしょう。実用に向けて超えるべきハードルはまだいくつもありますが、「無限の領域を理論的に扱える〝数学〟を活用したツールを使えば、要求通りに動くソフトウェアが作れるため、プログラムのバグが減り、短納期かつ低コスト化の厳しい顧客要求に応えられる高品質なソフトウェアが作れるだろう」と田原准教授は期待しています。

不具合を検知

このほか新しいソフトウェアとして、自己適応（self-adaptive）システムや、ウェブアプリケーション開発に用いるプログラミング言語であるPHP（Hypertext Preprocessor）の不具合を検知する技術なども開発しています。

自己適応システムは、状況の変化に応じて自らの構成や振る舞いを動的に変更するソフトウェアです。従来はサイバー攻撃などの予期せぬ障害が発生した場合、人手で修正する必要がありました。一例として、これをリアルタイム性の高いオンラインゲームに適用し、通信が遅延しても自律的に振る舞いを修正して快適なゲーム環境を作り出せることを確認しました。一方、PHPに関する技術はソフトウェアを動かさずに設定値のミスを検知するもので、実験ではウェブアプリケーションの設定ファイルとソフトウェア間の不適合を100％の確率で検出することに成功しています。（図1追加）

組み込みソフトウエアの検査もさらに、最近は企業と共同で組み込みソフトウェアのテストも実施しています。実際の機器にテストデータを入力し、プログラムにバグがないかを確かめる検査です。膨大な数のテストデータを従来よりも効率的に検査できる手法として確立しており、今後、あらゆる製造業に普及していく大きな可能性を秘めています。

【取材・文＝藤木信穂】